

The backtracking unit may also take corrective action by, for example, establishing a black hole host route to v as close as is possible to the source of the denial-of-service attack packets, and/or by establishing a special host route to v using the same next hop as an existing route, where the special host route tracking changes in the existing route 5 such that when a next hop for the existing route changes, the next hop for the host route changes similarly, and/or by establishing a rate-limit, for packets addressed to v, as close as is possible to the source of the denial-of-service attack packets.

BRIEF DESCRIPTION OF THE DRAWINGS

10 The above set forth and other features of the invention are made more apparent in the ensuing Detailed Description of the Invention when read in conjunction with the attached Drawings, wherein:

Fig. 1 is a simplified diagram of a data communications network and related components, including servers and routers;

15 Fig. 2 is a block diagram of a denial-of-service attack traceback unit in accordance with the teachings of this invention; and

Fig. 3 is a logic flow diagram depicting a method executed by the denial-of-service attack traceback unit of Fig. 2.

DETAILED DESCRIPTION OF THE INVENTION

It is first noted that in copending and commonly assigned U.S. Patent Application 20 09/_____, filed on even date herewith, entitled "Method for Protecting Web Servers Against Various Forms of Denial-of-Service Attacks", the inventor teaches several techniques for defending against an occurrence of a denial-of-service attack. The disclosure of this commonly assigned U.S. Patent Application is incorporated by reference herein in its entirety. It is further noted that the malicious traffic (e.g., denial-of-service attack) traceback teachings of this invention may be used in conjunction with the various techniques for protecting against such attacks disclosed in the commonly assigned Patent Application, as well as with other types of defensive mechanisms. For example, once a server or a firewall or a router determines that a denial-of-service attack is underway, and defensive mechanisms are deployed or are being deployed, the 25 30 teachings of this invention can be used to traceback to the source of the denial-of-service